

AB:OG

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

FILED UNDER SEAL

IN THE MATTER THE SEARCH OF:

**APPLICATION IN SUPPORT
OF A SEARCH WARRANT**

THE PREMISES KNOWN AND DESCRIBED AS
6622 FLEET STREET, APARTMENT 2J, FOREST
HILLS, NEW YORK 11375

19-MJ-439

----- X

I, DAMON GERGAR, being first duly sworn, hereby depose and state as
follows:

INTRODUCTION AND AGENT BACKGROUND

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS 6622 FLEET STREET, APARTMENT 2J, FOREST HILLS, NEW YORK 11375 (the “Subject Premises”), the items described in Attachment A to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 6622 FLEET STREET, APARTMENT 2J, FOREST HILLS, NEW YORK 11375 (the "Subject Premises"), further described in Attachment A, for the things described in Attachment B.

2. I am a detective employed by the New York Police Department and I have been a police officer for 19 years. I have been a detective for over 10 years, including being assigned to the Vice Major Case Squad for approximately 8 years and the Criminal Enterprise Investigation Section for 2 years as a Border Enforcement Security Task Force (BEST) officer with the Department of Homeland Security. My current responsibilities include investigating cases related to money laundering, contraband seizures, internal conspiracy, drug trafficking, human trafficking and cases involving the promotion of a sexual performance by a child through the use of electronic devices and the internet, possession and distribution of child pornography through the use of electronic devices and the internet, as well as dissemination of indecent material to minors, and other incidents of the exploitation of children on the internet. I have participated in the execution of over 100 search warrants in cases involving the exploitation of children on the internet and have participated in over 100 interviews involving subjects who have discussed the methods by

¹ Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

which they engage in the possession, storage and distribution of child pornography. I have worked as an investigating and arresting officer as well as a member of an investigative team assisting other detectives in my unit, with the Department of Homeland Security and the Federal Bureau of Investigation in the identification of persons involved in producing, collecting and trading of child pornography, the execution of search warrants, preliminary examination of computer data, and interviews of persons arrested for possession and/or promoting child pornography. I have received specialized training in the area of “on-line” criminal investigations, including the investigation of Internet sexual predators, and the production, possession, and distribution of still and video images depicting underage children engaged in sexual activity or sexual conduct, and/or the lewd depiction of the genitals of these underage children, especially when these illicit images are transmitted or received over the Internet. These investigations are commonly categorized by the term “child pornography.” I have received training in the area of computer evidence handling and computer forensics, including the ability to conduct forensically sound “field previews” of computers suspected of being involved in the aforementioned types of criminal activity. I have attended and successfully completed training courses provided by federal, state and private organizations in the identification of child pornography, identification of computer evidence, examination of computers and computer related material using forensically sound methods both on-site and in a laboratory environment. These courses have included: National White Collar Crime Center (NW3C) courses in Basic Data Recovery and Analysis, ICAC Peer to Peer Training Courses, FBI Image Scan Course, and Social Media Investigations. I am a licensed Peer to Peer investigator, licensed by TLO, Inc., the developers of the Child Protection System software. I

have attended the Basic Peer to Peer Investigations Course by TLO, Inc., the Gigatribe Training Course for licensed Peer to Peer Investigators given by TLO, Inc. I have attended courses sponsored by ICAC on conducting peer to peer investigations on Ares utilizing RoundUpAres, on the BitTorrent Network utilizing Torrential Downpour and on Freenet, utilizing Roundup Freenet. I have also worked with law enforcement officials in the investigation of crimes against children including special agents of the Child Exploitation Group of the Department of Homeland Security and the Innocent Images Project of the Federal Bureau of Investigation. I have attended the Forensic Imaging training given by the National Center for Missing and Exploited Children (NCMEC).

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

4. As alleged below, there is probable cause to believe that the Subject Premises contains evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant, and does not set forth all of my knowledge about this matter.

DEFINITIONS AND BACKGROUND

6. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

- a. The terms “minor,” “sexually explicit conduct,” and “visual depiction” are defined as set forth in Title 18, United States Code, Section 2256.
- b. The term “child pornography” is defined in Title 18, United States Code, Section 2256(8), in pertinent part, as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . .”²
- c. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.
- d. The term “IP Address” or “Internet Protocol Address” means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

² See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

c. The term “Internet” refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. The term “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

7. Peer to Peer (“P2P”) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others who are running compatible P2P software. There are several P2P networks currently operating, one of these being the “eDonkey” network (“eDonkey”).

8. P2P file sharing networks, including the eDonkey network, are frequently used to trade digital files of child pornography. These files include both image and movie files. P2P file sharing programs are a standard way to transfer files from one computer system to another while connected to a network, usually the Internet. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files.

9. Many P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files

by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

10. Based on my training and experience, I know the following about the operation of the eDonkey file-sharing network:

a. The eDonkey network is also known as the eDonkey2000 file-sharing network, or eD2k. Users of this network can simultaneously provide files to users while downloading files from other users.

b. The eDonkey network can be accessed by computers running several different client programs. These programs share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of the same client.

c. During the default installation of an eDonkey client, settings are established which configure the host computer to share files. Depending upon the eDonkey client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

d. Typically, a setting establishes the location of one or more directories or folders whose files are made available for distribution to other eDonkey users.

e. Typically, a setting controls whether or not other users of the network can obtain a list of the files being shared by the host computer.

f. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This

feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

g. Files on the eDonkey network are uniquely identified using MD4 root hash of a MD4 hash list of the file. This treats files with identical content but different names as the same, and files with different contents but the same name as different.

h. Files located in a user's shared directory are processed by the client software. As part of this processing, a MD4 root hash value is computed for each file in the user's shared directory.

i. The eDonkey network uses MD4 root hash values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses MD4 root hash values to ensure exact copies of the same file are used during this process.

j. The eDonkey software allows the user to search for pictures, movies and other files by entering descriptive text as search terms. These terms are typically processed by peers based upon the information about the files that had been sent by individual users.

k. Entering search terms into an eDonkey client returns a list of files and descriptive information including, in some client software, the associated MD4 root hash values.

l. A person is able to compare the MD4 root hash values of files being shared on the network to previously identified MD4 root hash values of any file, including child pornography. Using a publicly available eDonkey client a user can select the MD4 root hash value of a known file and attempt to receive it. Once a specific file is identified, the download process can be initiated. Once initiated, a user is presented with a list of users or IP addresses that have recently been identified as download candidates for that file. This allows for the detection and investigation of computers involved in possessing, receiving and/or distributing files of previously identified child pornography.

m. The IP addresses can be used to identify the location of these computers. A review of the MD4 root hash signatures allows an investigator to identify the files that are child pornography.

n. The MD4 (or Message-Digest Algorithm) is a cryptographic hash function. The digest length is 128 bits.

o. The returned list of IP addresses can include computers that are likely to be within this jurisdiction. The ability to identify the approximate location of these IP address is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, a recent association between a known file (based upon MD4 root hash comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

p. Once this association has been established, an investigator can attempt to download the file from the associated user or view the contents of the shared

directory. Depending upon several factors including configuration and available resources, it might not be possible to do either.

q. Depending on the associated user configuration and available peer resources a listing of the files being shared may be displayed. In order to obtain this list of files, a direct connection between the computers must occur. This list can be a partial listing of the shared files. The file list can only be obtained if the associated peer is connected to the network and running an eDonkey client at that moment.

By receiving either a file list or portions of a download from a specific IP address the investigator can conclude that a computer, likely to be in this jurisdiction, is running an eDonkey client and possessing, receiving and/or distributing specific and known visual depictions of child pornography.

11. Based on my involvement in the investigation, I know that law enforcement conducted this investigation using [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

12. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

PROBABLE CAUSE

13. Based on my involvement in the investigation, I know that this investigation was conducted using [REDACTED]. Using these programs, law enforcement officers identified the IP address 104.162.52.236 (the “Target IP Address”) as a “top” offender. This means the Target Subject has been observed with a high number of known child pornography files. Using these programs, I have monitored how often the Target Subject is online and actually sharing and/or possessing these files. I have observed the Target Subject online sharing and/or accessing known child pornography files between on or about November 27, 2018 and on or about May 1, 2019.

14. Based on my involvement in the investigation and conversation with other law enforcement officers, I know that the law enforcement software is able to scour the eDonkey network for IP addresses that have been sharing and/or possessing child pornography files known to law enforcement. I am able to monitor the Target Subject’s activity by looking at the Global Unique Identifier (“GUID”) attached to the eMule application the subject is using

when he connects to the eDonkey network. A GUID is assigned to the computer when a file sharing program (such as eMule or any other peer-to-peer file sharing platform) is placed onto the computer. This series of numbers and letters is unique to each computer running the program around the world. Should the computer be used to access the internet from a different IP address the GUID will remain the same as it is intrinsic to the computer system. Further, should the user of the computer update the file sharing program with a newer version, a new GUID will be assigned to the computer for the updated program.

15. Based on my involvement in the investigation and conversations with other law enforcement officers, I know that on or about May 1st, 2019, from the response in CPS to the query done for Queens, New York, law enforcement officers determined that the Target IP Address with a GUID of A40F1C1AE30E536DF3852B5213CE6FA2 (the “Target GUID”) was logged as possessing digital movie files on dates on or about April 12th, 2019 through on or about May 1, 2019, on the eDonkey network. These files are believed to be child pornography files with hash values associated with child pornography files known to law enforcement.

16. Based on my participation in the investigation and conversations with other law enforcement officers, I know that the other law enforcement officers directly connected to the target IP address numerous times between on or about March 7, 2019 and April 21, 2019, while utilizing law enforcement software and did receive full and/or partial child pornography videos from IP address 104.162.52.236. The following are 5 files that law enforcement downloaded directly from IP address 104.162.52.236. Your Affiant

reviewed the files downloaded. These files, which are available for the Court's review, are described as follows:

- a. Video File Name: Streetlolita 8Yr Brazil.avi, Ed2k hash value: 21FA4CE5D17C2C4D814EA875B1C3E29F. Partial download completed on 4/9 at 10:09 PM EST. Description: This video file is twenty-five (25) minutes and one (1) second in length. This video file depicts two prepubescent female children approximately 8-11 years of age dressed in two piece bathing suits dancing. Both of the female children undress in front of the camera until they are completely nude. The next scene depicts a nude adult male lying on his back on a bed, the adult male penetrates the mouths of both of the female children with his erect penis.
- b. Video File Name: She really knows how to do it.mp4, Ed2k has value: 70AB2E186F73D33592BC7A26F65B78E8. Complete download completed on 4/2/2019 at 8:17 PM EST. Description: This video file is one minute and 36 seconds. It depicts one prepubescent female walking in a living room of a house while fully nude. She then gets on her knees and performs fellatio on an unknown male penis. The child then proceeds to masturbate the man's penis until he starts masturbating himself. The girl then walks away from the man.
- c. Video File Name: Pthc 2018 Estefy sonrie chupa y culea en medio de lamentos.wmv, Ed2k hash value: 50678C87312EE60286B6DC85F3431B9A. Partial download on 4/7/08 at 7:08 AM EST. Description: This is a seven minute and four second video that shows a preteen female about 6-7 years of age perform oral sex on an adult male. The adult male then bends her over and anally rapes her.
- d. Video File Name: (PHANT) -- pedogirl - kelly 0216.mp4, Ed2k hash value: DF805C89921F17687CB76E0174ED99E5. Partial download on 3/14/19 at 11:55 PM. Description: This is a 2 minute and 11 second video file. The color video depicts two prepubescent female children, both under ten-years-of-age, laying on top of each other while nude. Both children are lying on their backs and the video begins while zoomed in on the genital area of both female children. The video then shows an adult male penis, which is erect, being rubbed against and

being placed into the genitals of both of the female children. The video then concludes with the children kissing each other, after changing positions so they are now lying chest to chest on each other.

- e. Video File Name: 8y (hard anal).mp4, Ed2k hash value: 1BBC55CCA5251C3B071045ADA59A1C83. Downloaded on 3/16/19 at 8:06AM. Description: This is a ten minute and 57 second movie file of a man rubbing the buttocks of a prepubescent 6-8 yr old girl lying face down on a red cloth on a wooden floor. The man strips the bottoms off the child and parts her legs. The Man pulls the child's buttocks apart lewdly displaying her genitals and anus to the camera. The video cuts to a close up of the child's anus and the man penetrates the child's anus with his erect penis.

17. Based on my participation in the investigation and my conversations with other law enforcement officers, I know [REDACTED] that the Target GUID was associated with the computer using the Target IP Address. I determined that the Target IP Address was being used by the P2P file sharing client using the Target GUID between at least on or about November 27, 2018 and on or about May 1, 2019.

18. Based on my participation in the investigation and my conversations with other law enforcement officers, I know that law enforcement officers using publicly available Internet websites determined that the Target IP Address, used to access the above described files, was owned by Spectrum/Charter Communications (ISP). In response to a subpoena issued on or about April 16, 2019, requesting subscriber information and IP logs corresponding to the specific dates and times that the Target IP Address accessed and/or shared known child pornography files, Spectrum/Charter Communications (ISP) provided information indicating that the Target IP Address was assigned to Lidra Joyce of 6622 Fleet

Street Apt 2J, Forest Hills, NY 11375-4168 (the “Subject Premises”), from on or about October 25, 2017, through the present.

19. On or about May 1, 2019, I conducted surveillance of the Subject Premises with another law enforcement officer. The location is a seven story, brick multi-unit residential apartment building. The entrance to the building is marked, “The Fleetwood 66-22” in gray letters with black trim above the front entrance of the building. There is a tenant list near the mailbox area inside the apartment building that shows “Joyce” living in apartment 2J. The Subject Premises is located on the third floor. The door to apartment 2J is pink and is marked 2J above the doorbell.

20. Based on the above facts, it is reasonable to conclude that a user of a computer located at the subject location is in possession of evidence related to the offenses of possessing a sexual performance by a child.

21. Based on the foregoing, I respectfully submit that there is probable cause to believe that the evidence related to the above-mentioned crimes may be found inside the subject location and within and upon computers, cellphones and any and all electronic devices, and other electronic devices capable of storing data, information, and images, and the electronic storage media recovered from the subject location.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

22. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact,

including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

23. I know that collectors of child pornography typically retain their materials and related information for many years.

24. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

25. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

26. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

27. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

TECHNICAL BACKGROUND

28. As described above and in Attachment B, this application seeks permission to search for documents constituting evidence, fruits or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A that might be found in the Subject Premises, in whatever form they are found. One form in which the documents might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

29. I submit that if a computer or storage medium is found on the the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space — that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media — in particular, the internal hard drives of computers — contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. For example, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

e. Based on the evidence that a computer connected to a P2P network through an IP address registered at the Subject Premises, there is reason to believe that there is a computer currently located on the Subject Premises.

30. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic “attribution” evidence that establishes how the computers were used, the purpose of their use, who used them, and

when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the Subject Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

31. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. This is true because of the time required for examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing

electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the Subject Premises could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Subject Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would authorize seizing, imaging, or otherwise copying computers and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not

limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

33. Because several people might share the Subject Premises as a residence, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.³

CONCLUSION

34. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the Subject Premises there exists evidence of one or more crimes. Accordingly, a search warrant is requested.

35. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it

³ As a matter of practice, HSI diligently reviews all electronic devices seized during a search warrant. If the device appears to belong to an innocent third party, HSI releases the device as soon as the device has been imaged and has been confirmed to be “clean,” *i.e.*, does not contain any contraband or evidence of a crime. Until a given electronic device has been examined, there is no way to determine whether it was used to facilitate the criminal conduct under investigation or whether items relevant to the investigation have been transferred to such device.

might alert the target(s) of the investigation at the Subject Premises to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

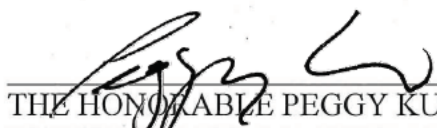
WHEREFORE, your deponent respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS 6622 FLEET STREET, APARTMENT 2J, FOREST HILLS, NEW YORK 11375.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court, in order to protect the integrity of the above-described investigation, to ensure that no target of this investigation flees, to ensure the integrity of evidence that may be recovered, and to ensure the safety of the agents and others.

TFO Det. D. G. #207

Task Force Officer Damon Gergar
Homeland Security Investigations

Sworn to before me this
9th day of May, 2019
10



THE HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A
Property to Be Searched

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

The Subject Premises are particularly described as a seven story, brick multi-unit residential apartment building. The entrance to the building is marked, “The Fleetwood 66-22” in gray letters with black trim above the front entrance of the building. There is a tenant list near the mailbox area inside the apartment building, ground floor, that shows “Joyce” living in apartment 2J. The subject location is located on the third floor. The door to apartment 2J is pink and is marked 2J above the doorbell. The building is located between Selfridge Street and Thornton Place.

ATTACHMENT B
Property to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;
2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:
 - a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.
7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
8. Records evidencing occupancy or ownership of the Subject Premises, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.
9. Records or other items which evidence ownership or use of computer equipment found in the Subject Premises, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.
10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.
11. Address books, names, lists of names and addresses of individuals believed to be minors.
12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.
13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.
14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers¹ or storage media² that contain records or information (hereinafter “COMPUTER”) used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A, including:
- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - f. evidence of the times the COMPUTER was used;
 - g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

¹ A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

² A “storage medium” for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - i. contextual information necessary to understand the evidence described in this attachment;
- 16. Records and things evidencing the use of the Internet Protocol address 104.162.52.236, including:
 - a. routers, modems, and network equipment used to connect computers to the Internet;
 - b. Internet Protocol addresses used by the COMPUTER;
 - c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
- 17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.